THOMAS F. CARLUCCI, CA Bar No. 135767
tcarlucci@foley.com
JAIME DORENBAUM, CA Bar No. 289555
jdorenbaum@foley.com
FOLEY & LARDNER LLP
555 CALIFORNIA STREET
SUITE 1700
SAN FRANCISCO, CA 94104-1520
TELEPHONE: 415.434.4484
FACSIMILE: 415.434.4507

DENNIS P. RIORDAN, CA Bar No. 69320
dennis@riordan-horgan.com
RIORDAN & HORGAN
523 OCTAVIA STREET
SAN FRANCISCO, CA 94102
TELEPHONE: 415.431-3472
FACSIMILE: 415.552.2703

Attorneys for Defendant
JING ZENG

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. JING ZENG, Defendant.	CASE NO. CR 16-00172 JD **DEFENDANT JING ZENG'S NOTICE OF MOTION AND MOTION TO DISMISS THE AMENDED INFORMATION, MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF** Date: October 26, 2016 Time: 9:30 am Courtroom: 2, 4th Floor, Oakland Judge: Honorable James Donato

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Federal Statutes

Federal Rules

Other Authorites

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on October 26, 2016 at 9:30 a.m. in the above-titled Court, Defendant Jing Zeng will and hereby does move this Court to dismiss all three counts in the amended information against him.

This motion is brought pursuant to Federal Rule of Criminal Procedure 12(b)(3) and is based on the grounds that the amended information fails to state the legally required elements for each of the three counts alleged against Mr. Zeng. This motion is supported by the following memorandum of points and authorities, the arguments of counsel, and such oral and documentary evidence that may be presented at the hearing of this motion.

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

Pursuant to Federal Rule of Criminal Procedure 12(b)(3), defendant Jing Zeng hereby moves to dismiss the amended information against him. The amended information purports to allege three offenses under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, but as to all three counts, it fails to state the legally required elements to sufficiently allege an offense.

The government initially filed a complaint against Mr. Zeng in August of 2015. The parties engaged in months of negotiations to resolve the case. Eventually, the government and the defense agreed on a rough set of facts that the government could likely prove; the government maintained that those facts constituted an offense under the CFAA, while the defense maintained that they did not. The parties agreed that they would file a stipulation, and the government would file an information reflecting the facts in the stipulation. The parties agreed that they would then make their respective legal arguments based on that stipulated information, and that this Court would then determine whether those facts constituted an offense.

The first information reflecting the stipulated facts was filed on April 22, 2016 (Dkt. 35.) It charged one felony count under the damage provision of the CFAA, 18 U.S.C. § 1030(a)(5)(A). Mr. Zeng filed his motion to dismiss the first information on June 13. (Dkt. 44.) That motion demonstrated

that, for numerous reasons, the stipulated facts did not constitute an offense.

After seeing the motion to dismiss, the government then apparently changed its mind about how to proceed with this case. Rather than responding, it filed an amended information. That information altered to some extent the factual allegations in the damage count, and it also added two new misdemeanor counts of unauthorized access of a computer in violation of § 1030(a)(2)(C).

These new allegations are still insufficient. The felony damage count, although slightly altered in the amended information, still suffers from the same core deficiencies that rendered the first information insufficient. The government will argue that the two new misdemeanor unauthorized access counts state an offense under the recent panel decision in *United States v. Nosal*, -- F.3d --, 2016 WL 3608752 (9th Cir. July 5, 2016) ("*Nosal II*"). But even were *Nosal II* valid precedent at this point in time, which it is not, the facts alleged here do not approach those that gave rise to criminal liability in *Nosal II* under a different provision of CFAA. Even assuming the truth of the government's own allegations, Mr. Zeng shared access with a third party in order to conduct speed tests for the benefit of his employer. Even if he did not have explicit permission to share the credentials, the government's allegations show that he had a mantle of authority to perform the tests, and he was not doing so for a forbidden purpose. Furthermore, the facts alleged in the amended information do not establish criminal liability on the part of the third party, so Mr. Zeng has none as an accomplice. The government's allegations thus fail to state an offense.

ARGUMENT

In this case as in other cases, the government continues to push for a nearly unlimited interpretation of the CFAA. But Congress never intended the CFAA to function as a general computer misuse statute. Rather, as the Ninth Circuit held in its seminal en banc opinion in *United States v. Nosal*, 676 F.3d 854 (9th Cir 2012) ("*Nosal I*"), the statute should generally be confined to its purpose of deterring and punishing hacking. In this case, the government does not allege any facts that even

resemble computer hacking.

Since Mr. Zeng filed his first motion to dismiss, the Ninth Circuit has decided two new cases regarding the CFAA—*United States v. Nosal*, -- F.3d --, 2016 WL 3608752 (9th Cir. July 5, 2016) ("*Nosal II*"), and *Facebook, Inc. v. Power Ventures, Inc.*, -- F.3d --, 2016 WL 3741956 (9th Cir. July 12, 2016). These cases sought to clarify the meaning of "without authorization" under the CFAA, but in reality, they muddied the waters. Both cases were the subject of intense criticism in the academic and popular press. The losing parties in both cases have filed petitions for rehearing en banc, and the Court has ordered the prevailing parties to respond in both cases. It is likely that the cases will not be resolved for months, and until then, neither *Facebook* nor *Nosal II* is final nor has precedential effect. *Carver v. Lehman,* 558 F.3d 869, 878 n.16 (9th Cir. 2009) ("[U]ntil the mandate issues, an opinion is not fixed as settled Ninth Circuit law, and reliance on the opinion is a gamble."); *accord NRDC v. Los Angeles*, 725 F.3d 1194, 1203 (9th Cir. 2013); *Comey v. Murphy Oil USA Inc.*, 718 F.3d 460, 468 (5th Cir. 2013); *United States v. Reyes*, 49 F.3d 63, 67-68 (2d Cir. 1995). More generally, the larger questions regarding the CFAA will persist until the Supreme Court or Congress intervene. In the meantime, however, the statute must be interpreted narrowly consistent with the rule of lenity and with the Ninth Circuit's guidance in *Nosal I*.

I. THE FELONY DAMAGE COUNT FAILS TO STATE AN OFFENSE

The government's felony damage count in the amended information remains deficient. As a factual matter, the amended information alleges slightly different facts than the original information, but the gist remains the same. As a legal matter, nothing has changed since April. Neither *Nosal II* nor *Power Ventures* dealt at all with the damage provision of the CFAA, so those cases have no effect on Count One of the amended information. For the sake of brevity, Mr. Zeng hereby incorporates by reference the arguments made in his first motion to dismiss, and only summarizes the key points here.

First, Count One fails to allege "damage" under the CFAA. The aim of the damage provision

was to "target[] conduct that denies privileges to other users, such as sending out computer viruses and launching denial-of-service attacks." Orin S. Kerr, *Computer Crime Law* 80 (2d ed. 2009). Consistent with that purpose, courts have held that "'damage' means actual harm to computer or networks" or destruction of data. *Custom Packaging Supply, Inc. v. Phillips*, 2016 WL 1532220 at *4 (E.D. Cal., April 15, 2016). Mere deletion of computer files does not constitute damage unless, at a minimum, the files were not "easily recoverable" and the "company had no duplicates" of those files. *See Int'l Airport Centers, LLC v. Citrin*, 440 F.3d 418, 419, 421 (7th Cir. 2006); *accord Dana Ltd. v. American Axle and Mfg.*, 2012 WL 2524008 at *5 (W.D. Mich. 2012).

In the amended information, the government alleges that Mr. Zeng installed a new operating system on his Mac laptop. Installing a new operating system is not "damage" of a computer, otherwise nearly every employee would become a criminal each time Apple comes out with an update. The government also alleges that Mr. Zeng "permanently remov[ed] certain items that had been originally installed by the company." (¶ 7.) But it does not specify at all what those items were, or that they were not easily recoverable. For example, if Mr. Zeng simply removed the licensed copy of Microsoft Word, then obviously Machine Zone could have re-installed the same software. Deleting "certain items" is not an offense.

The government makes no allegation that Mr. Zeng rendered the computer inoperable or altered anything on the computer that could not be easily undone by Machine Zone. It therefore fails to state an offense.

Second, the information fails to allege the requisite mens rea. The damage provision requires that the defendant act with the conscious object of causing the forbidden result—i.e., a damaged computer. *Oracle Corp. v. SAP AG*, 734 F. Supp. 2d 956, 964 (N.D. Cal. 2010). If a person installs a new operating system, for example, but does not realize that doing so will cause permanent deletion of irretrievable files, he does not commit an offense. It is only if he installs the new operating system with the purpose of causing permanent deletion of irretrievable files that a crime is committed. The

government in this case alleges that Mr. Zeng intentionally executed computer commands, but it does not allege that he did so with the purpose of causing damage.

Third, the information fails to allege the transmission element of § 1030(a)(5)(A). Merely erasing files using keystrokes or the computer's own internal software is not "transmission." *Citrin*, 440 F.3d at 419-20; *Dedalus Found. v. Banach*, 2009 WL 3398595 at *3 (S.D.N.Y. 2009). Rather, transmission requires external transfer—via virus, for example—of some code or command. The government makes no such allegation. It simply alleges that Mr. Zeng used "computer codes and commands," and read in context, it is clear that the government is referring to the Mac laptop's own internal codes and commands.

Fourth, even assuming the information successfully pleads the elements of a misdemeanor damage offense, it fails to allege the $5,000 loss element necessary for a felony offense. Money spent only counts as "loss" if it is a natural and foreseeable result of the defendant's conduct, and if it is reasonably necessary response. *United States v. Middleton*, 231 F.3d 1207, 1213 (9th Cir. 2000). In this case, the government merely alleges that Machine Zone spent more than $5,000 on investigation, but it makes no allegation that those expenditures were reasonable and necessary.

* * * *

It is notable that, even after seeing Mr. Zeng's first motion to dismiss, the government is still unable to plead a sufficient felony count. For example, if the government had any evidence to that effect, it could have simply alleged that the files deleted by Mr. Zeng "were not easily recoverable by Machine Zone." Those words, if added to the information, would at least have sufficiently pleaded that element of the offense. But it did not do so—presumably because it has no evidence supporting such an allegation.

In any event, regardless of what evidence the government has or does not have, the allegations contained in Count One fail to state an offense. The felony damage count should be dismissed.

II. THE MISDEMEANOR UNAUTHORIZED ACCESS COUNTS FAIL TO STATE AN OFFENSE

The amended information adds two additional counts of unauthorized access of a computer in violation of § 1030(a)(2)(C). The gist of these allegations is that, while he was still an employee of Machine Zone, Mr. Zeng shared his access credentials with a third party located in China. Count Two is based on one such incident in March 2015, while Count Three is based on another incident in July 2015. Both counts allege that Mr. Zeng instructed the third party to download a beta version of a new game so that it could be speed-tested on a Chinese cell phone.

The facts alleged in the amended information make clear that the government does not accuse Mr. Zeng of personally committing the purportedly forbidden act of access exceeding and without authorization—rather, the government alleges that Mr. Zeng is liable as an accomplice for assisting and instructing the third party in China to commit the crime.

Mr. Zeng will first review the relevant Ninth Circuit law addressing the issue of authorization, and will then demonstrate that the amended information fails to state a § 1030(a)(2)(C) misdemeanor offense for two independent reasons. First, the information fails to allege that the third party who actually accessed the computer committed a CFAA crime, because the information does not sufficiently allege either that the third party gained access in excess of, or without, authorization, or that the third party *knew* that he was acting without or in excess of authorization. That latter allegation that is of particular importance given that the third party's alleged conduct took place in China. It is doubtful that the CFAA could be applied extraterritorially absent such a mens rea requirement.

Second, the information likewise fails to sufficiently allege either that Mr. Zeng gained access in excess of, or without, authorization, or that Mr. Zeng knew that he was acting without or in excess of authorization.

A. The Relevant Law

1. *Unauthorized Access Under Nosal I*

The CFAA forbids accessing a computer "without authorization." Courts have struggled to

define that phrase. The issue comes up frequently in cases where a legitimate account holder shares his password and access credentials with a third party, who then accesses a computer without the computer owner's authorization.

For example, each time a person logs into facebook.com, she accesses Facebook's computers. Facebook's terms of service state explicitly that account holders may not share passwords with anyone else. Thus, when a mother logs into her son's Facebook account in order to check his social media usage, she does so with the permission of the account holder (her son) but not with the permission of the computer owner (Facebook). On the face of the statute, it is unclear whether the mother's conduct violates the CFAA. It depends on the meaning of "without authorization"—whether authorization can be granted only by the computer owner, or whether it can also be granted by the account holder.

In *Nosal I*, the Ninth Circuit stated that authorization can be granted by the account holder. In fact, the *Nosal I* en banc panel considered precisely the factual scenario above, that of a family member logging into a Facebook account in violation of the terms of service. 676 F.3d at 861. The *Nosal I* court held that such conduct cannot be considered an offense. It held that criminalizing such conduct would render the CFAA far broader than intended, and it therefore held that the CFAA must be limited to crimes akin to hacking—i.e., conduct that involves circumvention of technological access barriers. *Id.* at 862-63.

2. *Unauthorized Access Under Nosal II and Power Ventures*

The matter admittedly became more complicated after the Ninth Circuit's recent decisions in *Nosal II* and *Power Ventures*. Mr. Zeng submits that those decisions were incorrectly decided, are not final, and have no precedential effect unless and until mandate issues. *NRDC,* 725 F.3d at 1203. Mr. Zeng expects that they will be overturned by either the pending en banc proceedings or by the Supreme Court. Nonetheless, even under *Nosal II* and *Power Ventures*, the information here fails to state an offense.

The gist of *Power Ventures* and the majority opinion in *Nosal II* appears to be that password

sharing is sometimes a crime and sometimes not a crime under the CFAA. Unfortunately, the opinions are somewhat less than pellucid when it comes to defining the line between criminal and noncriminal conduct. As the *Nosal II* dissent pointed out, the majority failed to define its limiting principle with any clarity. 2016 WL 3608752 at *19-20 (Reinhardt, J., dissenting). Nonetheless, the opinions indicated suggested three limiting principles.

a. Revocation

First and foremost, the opinions suggested the revocation is the critical factor distinguishing innocuous password sharing from criminal password sharing. In *Nosal II*, the alleged criminals were former employees whose access credentials had been revoked, and they then borrowed credentials from a current employee. The majority suggested that the fact of revocation was centrally important: "once authorization to access a computer has been affirmatively revoked, the user cannot sidestep the statute by going through the back door and accessing the computer through a third party." 2016 WL 3608752 at *1. The majority referred to the fact of revocation repeatedly throughout its opinion, including in its attempt to distinguish *Nosal I*. *See, e.g.*, *id*. at *7 ("What *Nosal I* did not address was whether Nosal's access to Korn/Ferry computers *after* both Nosal and his co-conspirators had terminated their employment and Korn/Ferry revoked their permission to access the computers was "without authorization."); *id*. at *8 (stating that there is no authority "that a former employee whose computer access has been revoked can access his former employer's computer system and be deemed to act with authorization").

Power Ventures, decided one week later, relied on *Nosal II* and held that revocation was the critical fact in that case as well. Power Ventures operated a social media website that aggregated the content from other social media websites, including Facebook. In other words, using an account holder's password with her permission, it scraped content from Facebook and put it on its own website. 2016 WL 3741956 at *1-2. Facebook eventually discovered this conduct and sent Power Ventures a

cease and desist letter.

The Ninth Circuit held that it was the cease and desist letter that created liability. Prior to that letter, Power Ventures had permission from account holders, so "it did not initially access Facebook's computers 'without authorization' within the meaning of the CFAA." *Id*. at 7. But once the cease and desist letter came, however, the Ninth Circuit held that access was revoked—and only at that point did Power Ventures's continued access become unlawful. It. at *8-9. It was only the revocation and rescission that created liability.

The best reading of the majority opinion in *Nosal II* and *Power Ventures* is that sharing access credentials is forbidden if and only if the third party's access credentials have been explicitly revoked or rescinded.

b. "Mantle or Authority"

Nosal II also suggested a somewhat different limiting principle. It suggested, in other words, that because the account holder in that case had no "mantle or authority" to share her password with terminated employees, they were all guilty of a crime. Thus password sharing is a crime if and only if the password holder does not have the "mantle or authority" to share her password. 2016 WL 3608752 at *8.

c. Knowledge of Authorization

In order to commit the crime of unauthorized access under the CFAA, a person must be aware that he lacks authorization to access the protected computer. As the Ninth Circuit suggested in *Power Ventures*, the defendant there was only guilty once it "*knew* that it no longer had authorization to access Facebook's computers" and then "*deliberately* disregarded the cease and desist letter." *Id*. at *7-8 (emphases added). It was guilty because it "intentionally accessed Facebook's computers *knowing that it was not authorized to do so*." *Id*. at *8 (emphasis added). In fact, at the oral argument in *Nosal II*, counsel for the government argued that knowledge of lack of authorization on the part of *both* the person

sharing his access code or credential *and* the person to whom he provides the credential is the critical fact on which liability depends.[1] In short, even though *Power Ventures* expands liability beyond what *Nosal I* allowed, it still predicated liability on a person's *subjective knowledge* that he lacks authorization.

That mens rea requirement is particularly germane in an international case such as this one. The core criminal conduct alleged by the principals took place in China. In this case, the information alleges that a third party in China used a cell phone to access Machine Zone computers (and it does not specify where those computers were located). "[L]egislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States." *EEOC v. Arabian Am. Oil Co*., 499 U.S. 244, 248 (1991) (quoting *Foley Bros., Inc. v. Filardo*, 336 U.S. 281, 285 (1949)). And as the Supreme Court clarified more recently, courts cannot assume that a statute has extraterritorial effect unless Congress gives very clear indication of its intent to do so. "When a statute gives no clear indication of an extraterritorial application, it has none." *Morrison v. Nat'l Australia Bank Ltd*., 561 U.S. 247, 255 (2010); *accord United States v. Chao Fan Xu*, 706 F.3d 965, 974 (9th Cir. 2013).

It is unclear whether the CFAA has extraterritorial application. But were the CFAA to be interpreted to impose strict liability on foreign citizens on foreign soil who gain access to computers, be they in the United States or abroad, while those foreigners are unaware that they lack the legal authority to gain such access, the CFAA would be subject to constitutional challenge on vagueness and due process notice grounds. *See United States v. Lanier*, 520 U.S. 259, 266-67 (1997).

B. The Misdemeanor Unauthorized Access Counts Must Be Dismissed Because the Information Fails to Allege an Offense by the Alleged Principals

Mr. Zeng's alleged liability in Counts Two and Three is predicated on principles of accomplice liability. It was the third party who allegedly accessed Machine Zone's computers without

[1] The oral argument in *Nosal II*, which took place on October 20, 2015, can be found on the Ninth Circuit's website. The cited portion of the government's argument can be found at minutes 42:35 to 43:00.

authorization—Mr. Zeng allegedly assisted by providing access credentials. But it is an elementary principle of accomplice liability that the accomplice is not guilty unless it is proven that the principal committed a crime. *See* 2 LaFave, *Substantive Criminal Law* § 13.3 (2d ed. & 2016 West Update) ("If the acts of the principal in the first degree are found not to be criminal, then the accomplice may not be convicted.").

Put differently, in order to prove accomplice liability, the government must prove "that someone committed the underlying substantive offense." *United States v. Thum*, 749 F.3d 1143, 1149 (9th Cir. 2014) (internal quotation marks omitted); *see also* Ninth Circuit Manual of Model Criminal Jury Instructions 5.1 (stating that the first element of accomplice liability is "[a crime] was committed by someone"); The government need not formally charge the principal, and the jury can find an accomplice guilty regardless of whether the principal is charged or convicted. It need not even identify the principal—but it nonetheless must prove that some principal committed the underlying offense. *Feldstein v. United States*, 429 F.2d 1092, 1095 (9th Cir. 1970).

Under a straightforward reading of *Nosal I*, the third parties did not commit any crime, because under a straightforward reading of *Nosal I*, consensual sharing of access credentials does not give rise to liability. But even assuming that the principles set forth in *Nosal II* and *Power Ventures* remain good law, the principals are still not guilty of an offense on the government's own allegations.

As described above, *Nosal II* and *Power Ventures* suggest that sharing access credentials if and only if permission has been previously revoked for the person who accesses the computer. In this case, there is no allegation of revocation. There is no allegation that Machine Zone had revoked any credentials of the third parties in China (or that it had revoked Mr. Zeng's credentials). Therefore, for this reason, Counts Two and Three fail to state an offense as to the alleged principals.

Furthermore, as demonstrated above, *Power Ventures* holds, and the government agreed in *Nosal II*, that liability only attaches where a person accesses a computer knowing that he does not have permission to do so. There is no such allegation here. That failure negates liability for both the third

parties and Mr. Zeng. Even where an accomplice has the forbidden mental state, no accomplice liability attaches where the "individual in the role of a principal . . . is not really committing a crime because he (unlike the accomplice) does not have the mental state required for commission of the offense." 2 LaFave, *supra*, § 13.3(c).

Here, the information does not allege that the principals have the requisite mental state for the alleged offense. There is no allegation that the third parties in China had any knowledge that they lacked authorization. In fact, the allegations suggest quite the opposite. They received permission to access Machine Zone computers from an executive at Machine Zone, Mr. Zeng. Even assuming arguendo that Mr. Zeng did not have *actual* authority to confer that authorization, he at least had *apparent* authority. Because there is no allegation that the third parties knew they lacked authorization, the information fails to state facts constituting an offense by the third parties. Because the information fails to state an offense by the third party principals, it also fails to state an offense by Mr. Zeng. Because there is no principal liability, there is no derivative liability either.

The Ninth Circuit's decision in *Thum* is instructive. The defendant there was charged with alien smuggling crimes, namely encouraging aliens to unlawfully reside in the United States. 749 F.3d at 1144-45. One of the government's theories was that Thum was liable because he assisted a smuggler named Chaplain. But the Ninth Circuit held that the government's accomplice theory against Thum was fatally flawed because it could not prove that Chaplain committed the underlying offense. Although Chaplain was admittedly a smuggler who transported aliens over the border, there was no evidence that Chaplain encouraged those aliens to reside illegally in the United States. *Id*. at 1148-49. Because Chaplain was not proven to be guilty of the underlying offense, Thum was not guilty of aiding that offense.

The result here is the same as in *Thum*. Given the limiting principles stated above, the information here fails to allege that the principal or principals—i.e., the third parties in China—committed the underlying offense of unauthorized access. Mr. Zeng has no liability as an accomplice.

C. The Amended Information Fails to Adequately Allege a § 1030(a)(2)(C) Offense Against Mr. Zeng.

The information alleges that Mr. Zeng shared his credentials so that a third party could test a Machine Zone game on a Chinese cell phone. According to the information, the third party in China accessed Machine Zone computers without Machine Zone's consent but with Mr. Zeng's consent. But under *Nosal I*, password sharing alone is not a crime. Authorization can be conferred by either the computer owner or by the account holder. Therefore, the allegations in Count Two and Three fail to state an offense.

Furthermore, there is no allegation that Mr. Zeng was doing so for an impermissible purpose or for his own benefit. In fact, the allegations suggest that he was sharing his credentials for the company's benefit. For that matter, there is not even an allegation that Machine Zone objected to the procedure. But in any event, as an operations engineer and executive at Machine Zone, Mr. Zeng had the "mantle or authority" to share his credentials for the purpose of testing Machine Zone products. The information fails to allege any facts to the contrary. Nor does it allege that the third parties who were enlisted to speed-test the games had any impermissible purpose or received any impermissible benefit. It therefore fails to allege an offense.

Additionally, the reasons why the information fails to state an offense against the third party principal who gained access to the Machine Zone computer apply to Mr. Zeng as well. He did not give his access credentials to a party whose authorization to enter that computer had been revoked, as was the case in *Nosal II*. And the information contains no allegation that either the third party principal or Mr. Zeng subjectively knew that the third party's accessing of the Machine Zone computer was unauthorized.

Both *Nosal II* and *Power Ventures* insist there are limitations on the reach of CFAA, and under those limiting principles, Counts Two and Three do not state an offense.

CONCLUSION

The amended information adds some additional facts, but it is still deficient. The government has once again failed to allege offenses under the CFAA, and so all counts of the amended information should be dismissed.

Date: September 21, 2016

s/ Thomas F. Carlucci

THOMAS F. CARLUCCI

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document has been served to all counsel of record, listed below, who are deemed to have consented to electronic service via the Court's CM/ECF system per Civil L.R 5-1. The undersigned further certifies that a true and correct copy of the foregoing document has been served via mail and e-mail on the counsel of record who are not registered participants of the CM/ECF system, listed below.

I declare under penalty of perjury of the laws of the United States of America that the foregoing is true and correct.

Executed on September 21, 2016.

/s/ Thomas F. Carlucci

THOMAS F. CARLUCCI

ELECTRONIC MAIL NOTICE LIST

Candace Kelly Candace.Kelly@usdoj.gov, rosario.calderon2@usdoj.gov

John Henry Hemann john.hemann@usdoj.gov, jacquelyn.lovrin@usdoj.gov

COURTESY COPY

Chambers Copy
James Donato
United States Magistrate Judge Chief
Clerk's Office
San Francisco Courthouse
450 Golden Gate Ave.
San Francisco, CA 94102
Case No. CR 16-00172 JD